



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,706	08/28/2001	Deepak Gupta	JP920010196US1	5753
39903	7590	02/07/2007	EXAMINER	
ANTHONY ENGLAND			ABRISHAMKAR, KAVEH	
PO Box 5307			ART UNIT	
AUSTIN, TX 78763-5307			PAPER NUMBER	
			2131	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		02/07/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/940,706

Applicant(s)

GUPTA, DEEPAK

Examiner

Kaveh Abrishamkar

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 February 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on February 3, 2005. Claims 1-15 have all been amended per the received amendment. No claims were cancelled. Claims 1-15 are currently pending consideration.

Response to Arguments

2. Applicant's arguments filed February 3, 2005 have been fully considered but they are not persuasive for the following reasons:

The Applicant does not make specific arguments regarding the independent claims 1,6, and 11, and therefore, the newly added limitations will be addressed in the rejection given below. Regarding claims 2,4,7,9,12, and 14, the Applicant argues that the Cited Prior Art (CPA), Datar et al. (U.S. Patent 6,351,812), does not teach that the second type of access is responsive to additional authentication data. This is not persuasive. Datar teaches that first the certificate status cookie is used to establish that the certificate is valid (column 6 lines 28-47), and then if the participant is seeking access to a status-restricted application, there is a request for an Associate Status Cookie, which defines the participants' status (column 8 lines 8-18). This is seen as an additional authentication step, and therefore, the arguments are not found persuasive. Furthermore, the Applicant argues that the CPA does not teach invalidating a previously identified certificate, and that a second computer receives a new certificate, and that

Art Unit: 2131

that there is a command to replace the invalid certificate. These arguments are not found persuasive. A client tries to access an application and presents a certificate status cookie, and if the cookie states that the certificate is not longer valid, the user is not allowed to access the application with that current certificate (invalidated) (column 7 lines 42-50). Furthermore, the application directly issues an inquiry to a CSA and obtains a fresh cookie and forwards it to the client (column 7 lines 42-54). Therefore, the Datar reference is maintained for the limitations that are specifically argued by the Applicant.

Claim Objections

3. Claims 2,4,5 are objected to because of the following informalities: The previously mentioned claims all contain the "improved method" though the independent claim 1 has no mention of an "improved" method. Therefore, it is recommended that the word improved be removed from these claims. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2131

4. Claims 1 - 15 are rejected under 35 U.S.C. 102(e) as being anticipated by Datar et al. (U.S. Patent 6,351,812).

Regarding claim 1, Datar discloses:

A method for providing secure authentication, the method comprising:

a) receiving basic authentication data from a first computer for a secure transaction between the first computer and a second computer, wherein the receiving is by the second computer, the secure transaction is during a certain communication session between the first and second computer, and the basic authentication data has been certified by an accepted certifying authority, and wherein the basic authentication data includes a public key of the first computer for permitting a first type of access by the first computer to an application provided by the second computer, (column 5 line 47 – column 6 line 13), *wherein the basic authentication data is interpreted as the client sending his/her identity and the public key to a Certificate authority, which is issued a certificate, which is then used for communicating from the client (first computer) to an application (second computer) by placing a certificate status cookie in a browser which includes a plurality of attributes used to validate the client's certificate to the application (second computer) (column 6 lines 38-48);*

b) storing a copy of the first computer's public key (column 7 lines 18-31), *wherein the second computer issues a challenge encrypted with the public key to the client;*

Art Unit: 2131

c) requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual data unit is for permitting a second type of access by the first computer to an application provided by the second computer (column 8 lines 31-65), *wherein certain applications which are status-restricted require an associate status cookie which supplies the status of the client to the second computer,*

d) receiving the additional authentication data unit by the second computer from the first computer (column 8 lines 31-65), *wherein certain applications which are status-restricted require an associate status cookie which supplies the status of the client to the second computer, and*

e) verifying authenticity of the additional individual authentication data unit, wherein c) includes storing the first computer's public key by the second computer during the certain communications session, and the verifying includes verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second computer obtaining another copy of the public key (column 8 lines 8-30), *wherein there is a digital signature of the attributes of the associate status cookie, which is verified using the public key of the client.*

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Datar discloses:

Art Unit: 2131

The improved method as claimed in claim 1 wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase (paragraph 9 lines 24-34).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Datar discloses:

The method as claimed in claim 1, wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority (column 8 lines 8-30), *wherein there is a digital signature of the attributes of the associate status cookie, which is verified using the public key of the client.*

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Datar discloses:

The improved method as claimed in claim 1 wherein the second type of access includes an access for an application in which an email message is securely transmitted (column 9 lines 10-18).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Datar discloses:

The improved method as claimed in claim 1, wherein the authentication data includes an identity certificate, and the method includes:

receiving, by the second computer, a command from the first computer for the second computer to invalidate a previously presented identity certificate (column 7 lines 32-43), *wherein if the cookie containing the certificate is invalid, the client is redirected to get a new cookie (certificate information); and*

receiving, by the second computer, a new identity certificate from the first computer to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session (column 7 lines 41-64), *wherein the client is redirected to get a new cookie (with certificate attributes) and then is redirected to the application (second computer) with the new cookie (certificate).*

Regarding claim 6, Datar discloses:

A system for providing secure authentication, the system comprising:

means for receiving basic authentication data from a first computer for a secure transaction between the first computer and a second computer, wherein the receiving is by the second computer, the secure transaction is during a certain communication session between the first and second computer, and the basic authentication data has been certified by an accepted certifying authority, and wherein the basic authentication data includes a public key of the first computer for permitting a first type of access by the first computer to an application provided by the second computer, (column 5 line 47 – column 6 line 13), *wherein the basic authentication data is interpreted as the client sending his/her identity and the public key to a Certificate authority, which is issued a certificate, which is then used for communicating from the client (first computer) to an application (second computer) by placing a certificate status cookie in a browser which includes a plurality of attributes used to validate the client's certificate to the application (second computer) (column 6 lines 38-48);*

Art Unit: 2131

means for storing a copy of the first computer's public key (column 7 lines 18-31), *wherein the second computer issues a challenge encrypted with the public key to the client;*

means for requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual authentication data unit is for permitting a second type of access by the first computer to an application provided by the second computer (column 8 lines 31-65), *wherein certain applications which are status-restricted require an associate status cookie which supplies the status of the client to the second computer;*

means for receiving the additional individual authentication data units by the second computer from the first computer (column 8 lines 31-65), *wherein certain applications which are status-restricted require an associate status cookie which supplies the status of the client to the second computer;* and

means for verifying authenticity of the additional individual authentication data unit, wherein the storing means includes means for storing the first computer's public key by the second computer during the certain communication session, and the means for verifying includes means for verifying the additional individual authentication data unit by the second computer during the certain communication session, and the means for verifying includes means for verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second

Art Unit: 2131

computer obtaining another copy of the public key (column 8 lines 8-30), *wherein there is a digital signature of the attributes of the associate status cookie, which is verified using the public key of the client.*

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Datar discloses:

The system as claimed in claim 6 wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase (paragraph 9 lines 24-34).

Claim 8 is rejected as applied above in rejecting claim 6. Furthermore, Datar discloses:

The system as claimed in claim 6, wherein the authenticity of said additional individual authentication data is established by means of signature of said accepted certifying authority (column 8 lines 8-30), *wherein there is a digital signature of the attributes of the associate status cookie, which is verified using the public key of the client.*

Claim 9 is rejected as applied above in claim 6, wherein the second type of access includes an access for an application in which an email message is securely transmitted (column 9 lines 10-18).

Claim 10 is rejected as applied above in rejecting claim 6. Furthermore, Datar discloses:

The system as claimed in claim 6, wherein the authentication data includes an identity certificate, and the system includes:

means for receiving, by the second computer, a command from the first computer for the second computer to invalidate a previously presented identity certificate (column 7 lines 32-43), *wherein if the cookie containing the certificate is invalid, the client is redirected to get a new cookie (certificate information);* and

means for receiving, by the second computer, a new identity certificate from the first computer to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session (column 7 lines 41-64), *wherein the client is redirected to get a new cookie (with certificate attributes) and then is redirected to the application (second computer) with the new cookie (certificate).*

Regarding claim 11, Datar discloses:

A computer program product comprising computer readable medium code stored on a computer readable storage medium embodied therein for providing secure authentication, the computer program product comprising:

computer readable program code means configured for receiving basic authentication data from a first computer for a secure transaction between the first computer and a second computer, wherein the receiving is by the second computer, the secure transaction is during a certain communication session between the first and second computer, and the basic authentication data has been certified by an accepted

Art Unit: 2131

certifying authority, and wherein the basic authentication data includes a public key of the first computer for permitting a first type of access by the first computer to an application provided by the second computer (column 5 line 47 – column 6 line 13), *wherein the basic authentication data is interpreted as the client sending his/her identity and the public key to a Certificate authority, which is issued a certificate, which is then used for communicating from the client (first computer) to an application (second computer) by placing a certificate status cookie in a browser which includes a plurality of attributes used to validate the client's certificate to the application (second computer) (column 6 lines 38-48);*

computer readable medium code means configured for storing a copy of the first computer's public key (column 7 lines 18-31), *wherein the second computer issues a challenge encrypted with the public key to the client;*

computer readable program code means configured for requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual authentication data unit is for permitting a second type of access by the first computer to an application provided by the second computer (column 8 lines 31-65), *wherein certain applications which are status-restricted require an associate status cookie which supplies the status of the client to the second computer;*

computer readable program code means configured for receiving the additional individual authentication data units by the second computer from the first computer (column 8 lines 31-65), *wherein certain applications which are status-restricted require*

Art Unit: 2131

an associate status cookie which supplies the status of the client to the second computer, and

computer readable program code means for verifying authenticity of the additional individual authentication data unit, wherein the computer readable program code means configured for storing a copy of the first computer's public key includes computer readable program code means configured for storing the first computer's public key by the second computer during the certain communication session, and the verifying includes verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second computer obtaining another copy of the public key (column 8 lines 8-30), *wherein there is a digital signature of the attributes of the associate status cookie, which is verified using the public key of the client.*

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Datar discloses:

The computer program product as claimed in claim 11, wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase (paragraph 9 lines 24-34).

Claim 13 is rejected as applied above in rejecting claim 11. Furthermore, Datar discloses:

Art Unit: 2131

The computer program product as claimed in claim 11, wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority (column 8 lines 8-30), *wherein there is a digital signature of the attributes of the associate status cookie, which is verified using the public key of the client.*

Claim 14 is rejected as applied above in rejecting claim 11. Furthermore, Datar discloses:

The computer program product as claimed in claim 11, wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase (paragraph 9 lines 24-34).

Claim 15 is rejected as applied above in rejecting claim 11. Furthermore, Datar discloses:

The computer program product as claimed in claim 11, wherein the authentication data includes an identity certificate, and the computer program product includes:

computer readable program code means configured for receiving, by the second computer, a command from the first computer for the second computer to invalidate a previously presented identity certificate (column 7 lines 32-43), *wherein if the cookie containing the certificate is invalid, the client is redirected to get a new cookie (certificate information); and*

computer readable program code means configured for receiving, by the second computer, a new identity certificate from the first computer to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session (column 7 lines 41-64), *wherein the client is redirected to get a new cookie (with certificate attributes) and then is redirected to the application (second computer) with the new cookie (certificate).*

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.


Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Y.A. 2/01/07
KA
2/01/2007


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100